E P U B L I Q U E F R A A I S E

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

PCT/FR99/02608

REC'D 22 NOV 1999
WIPO PCT

BREVET D'INVENTION

FR99/2608

CERTIFICAT D'UTILITÉ - CERTIFICAT D'ADDITION

COPIE OFFICIELLE

Le Directeur général de l'Institut national de la propriété industrielle certifie que le document ci-annexé est la copie certifiée conforme d'une demande de titre de propriété industrielle déposée à l'Institut.

Fait à Paris, le 08 NOV. 1999

Pour le Directeur général de l'Institut
national de la propriété industrielle
Le Chef du Département des brevets

Martine PLANCHE

DOCUMENT DE PRIORITÉ

PRÉSENTÉ OU TRANSMIS
CONFORMÉMENT À LA REGLE
17.1.a) OU b)

INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE
SIEGE
26 bis, rue de Saint Petersbourg
75800 PARIS Cédex 08
Téléphone : 01 53 04 53 04
Télécopie : 01 42 93 59 30

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

26 bis, rue de Saint Pétersbourg
75800 Paris Cedex 08
Téléphone : 01 53 04 53 04 Télécopie : 01 42 93 59 30

BREVET D'INVENTION, CERTIFICAT D'UTILITE

Code de la propriété intellectuelle - Livre VI

REQUÊTE EN DÉLIVRANCE

cerfa N° 55-1328

Confirmation d'un dépôt par télécopie ☐

Cet imprimé est à remplir à l'encre noire en lettres capitales

Réservé à l'INPI

DATE DE REMISE DES PIÈCES 05 NOV 1998
N° D'ENREGISTREMENT NATIONAL 98 13938
DÉPARTEMENT DE DÉPÔT 75
DATE DE DÉPÔT 05 NOV. 1998

1 NOM ET ADRESSE DU DEMANDEUR OU DU MANDATAIRE À QUI LA CORRESPONDANCE DOIT ÊTRE ADRESSÉE

CABINET BALLOT-SCHMIT
7, rue Le Sueur
75116 PARIS
FRANCE

n°du pouvoir permanent / références du correspondant : SM/ 014267 — téléphone : 01.40.67.11.99

2 DEMANDE Nature du titre de propriété industrielle

☒ brevet d'invention ☐ demande divisionnaire ☐ certificat d'utilité ☐ transformation d'une demande de brevet européen

demande initiale : ☐ brevet d'invention ☐ certificat d'utilité n° date

Établissement du rapport de recherche ☐ différé ☒ immédiat

Le demandeur, personne physique, requiert le paiement échelonné de la redevance ☐ oui ☒ non

Titre de l'invention (200 caractères maximum)

SYSTEME DE PERSONNALISATION DE CARTES A PUCE.

3 DEMANDEUR (S) n° SIREN 7 4 9 7 1 1 2 0 0 code APE-NAF

Nom et prénoms (souligner le nom patronymique) ou dénomination

GEMPLUS

Forme juridique

Société en Commandite par par Actions

Nationalité (s) Française

Adresse (s) complète (s) Pays

Avenue du Pic de Bertagne
Parc d'activités de la Plaine de Jouques
13420 GEMENOS

FRANCE

En cas d'insuffisance de place, poursuivre sur papier libre ☐

4 INVENTEUR (S) Les inventeurs sont les demandeurs ☐ oui ☒ non Si la réponse est non, fournir une désignation séparée

5 RÉDUCTION DU TAUX DES REDEVANCES ☐ requise pour la 1ère fois ☐ requise antérieurement au dépôt ; joindre copie de la décision d'admission

6 DÉCLARATION DE PRIORITÉ OU REQUÊTE DU BÉNÉFICE DE LA DATE DE DÉPÔT D'UNE DEMANDE ANTÉRIEURE

pays d'origine	numéro	date de dépôt	nature de la demande

7 DIVISIONS antérieures à la présente demande n° date n° date

8 SIGNATURE DU DEMANDEUR OU DU MANDATAIRE (nom et qualité du signataire)

Paul BALLOT
92-1009
CABINET BALLOT SCHMIT

SIGNATURE DU PRÉPOSÉ À LA RÉCEPTION

SIGNATURE APRÈS ENREGISTREMENT DE LA DEMANDE À L'INPI

INPI
INSTITUT NATIONAL DE LA PROPRIETE INDUSTRIELLE

DIVISION ADMINISTRATIVE DES BREVETS

26bis, rue de Saint-Pétersbourg
75800 Paris Cédex 08
Tél. : 01 53 04 53 04 Télécopie : 01 42 93 59 30

SM/ 014267

BREVET D'INVENTION, CERTIFICAT D'UTILITE

DÉSIGNATION DE L'INVENTEUR
(si le demandeur n'est pas l'inventeur ou l'unique inventeur)

N° D'ENREGISTREMENT NATIONAL

9813938

TITRE DE L'INVENTION :

SYSTEME DE PERSONNALISATION DE CARTES A PUCE.

LE(S) SOUSSIGNÉ(S)

Cabinet BALLOT SCHMIT
7, rue Le Sueur
75116 PARIS
FRANCE

DÉSIGNE(NT) EN TANT QU'INVENTEUR(S) (indiquer nom, prénoms, adresse complète et de préférence le nom patronymique) :

MAUREL Frédéric

domicilié (s) au :

Cabinet BALLOT SCHMIT
7, rue Le Sueur
75116 PARIS
FRANCE

NOTA : A titre exceptionnel, le nom de l'inventeur peut être suivi de celui de la société à laquelle il appartient (société d'appartenance) lorsque celle-ci est différente de la société déposante ou titulaire.

Date et signature (s) du (des) demandeur (s) ou du mandataire

Paris, le 4 novembre 1998

Paul BALLOT - 92-1009
Cabinet BALLOT SCHMIT

BA 113/271196

SYSTEME DE PERSONNALISATION DE CARTES A PUCE

L'invention concerne les cartes à puce et, plus particulièrement, un système pour personnaliser en grande série les cartes à microcircuit.

Par carte à microcircuit, on entend une carte plastique dans l'épaisseur de laquelle est logé un microcircuit. Selon l'usage de la carte, il est nécessaire d'enregistrer des données issues d'un fichier de données et de calculs dans la mémoire d'un microcircuit notamment une puce avec ou sans microprocesseur. Ces opérations s'appellent "personnalisation" de la carte à microcircuit et sont réalisées par une machine de personnalisation. Le temps pour réaliser ces opérations est compris entre 15 et 30 secondes par carte pour des cartes utilisées dans le téléphone mobile par exemple.

Ces opérations sont réalisées par une machine comprenant plusieurs lignes ou appareils de personnalisation en parallèle qui comprennent chacun un lecteur/encodeur dans lequel le programme de personnalisation est téléchargé et qui fonctionne de manière autonome grâce à un microprocesseur.

Les données personnalisées de chaque carte sont fournies au lecteur/encodeur par un dispositif périphérique via un bus de communication associé à un dispositif de contrôle.

Or, pour tenir compte des aspects de sécurité, il est nécessaire d'assurer des fonctions supplémentair s, telles que :

- le calcul de clés dites de transport pour débloquer le microcircuit avant les opérations de personnalisation,
- le calcul d'une clé de session pour la sécurisation des données à introduire dans la carte et,
- le calcul d'un certificat qui autorise la création d'un répertoire ou d'un fichier.

Ces fonctions impliquent un dialogue entre chaque appareil de personnalisation et un dispositif périphérique, notamment pour chaque création de fichier ou répertoire, d'où un échange de données très important.

Actuellement, ces échanges de données sont effectués par l'intermédiaire d'un bus de communication qui connecte chaque appareil, poste ou ligne de personnalisation à un dispositif périphérique de cryptage capable de calculer les certificats permettant la création de chaque fichier et ce pour chaque carte. Or, la capacité du bus est insuffisante pour gérer un tel volume d'échanges de données.

Un but de la présente invention est donc de réaliser un système de personnalisation de cartes à puce, qui ne présente pas les limitations des systèmes de l'art antérieur, en améliorant les flux d'échanges de données entre les lignes ou appareils de personnalisation et les dispositifs périphériques de cryptage.

Ce but est atteint en mettant en oeuvre une architecture de communication entre les appareils ou lignes de personnalisation et les dispositifs périphériques dans laquelle, d'une part, les lignes de personnalisation reçoivent des données de personnalisation par un bus de communication et, d'autre part, un serveur de données fournit les données de cryptage aux lignes de personnalisation par des liaisons informatiques, les données de cryptage étant fournies par des dispositifs périphériques de cryptage via des liaisons informatiques.

Cette architecture permet de limiter le trafic de données sur le bus de communication en l'affectant aux données de personnalisation, les données de cryptage étant véhiculées par d'autres liaisons informatiques.

Par ailleurs, dans l'art antérieur, chaque poste de personnalisation est conçu pour solliciter un serveur de données de façon prédéterminée.

L'inconvénient réside dans le risque de requête d'un serveur de données par deux ou plusieurs postes de personnalisation en même temps alors qu'un autre serveur de données est disponible. Cela provoque une attente dans la tâche du poste de personnalisation.

L'invention a donc également pour but d'optimiser le temps de réponse d'un serveur de données à une requête d'un poste de personnalisation.

Ce but est atteint en ayant recours à un moyen interface de gestion, disposé entre les machines de personnalisation et les serveurs, qui soit informé et qui tienne compte de la disponibilité d'un serveur pour répondre au plus vite à la requête d'un poste de personnalisation.

L'invention concerne un système de personnalisation de cartes à puce caractérisé en ce qu'il comprend :

- au moins une machine de personnalisation équipée chacune d'au moins un poste de personnalisation émettant des requêtes en données de personnalisation ;
- au moins un serveur de données de personnalisation délivrant des données de personnalisation ;
- au moins une interface de gestion connectée d'une part à l'une au moins desdites machines de personnalisation et d'autre part à l'un au moins desdits serveurs de données par une liaison bi-directionnelle, ladite interface de gestion recevant lesdites requêtes, les transmettant à un au moins desdits serveurs, réceptionnant la réponse correspondante, et la transmettant au poste de personnalisation requérant,

caractérisé en ce que ladite interface de gestion est apte à gérer la transmission des sollicitations/requêtes ou besoins en données de personnalisation à l'un au moins desdits serveurs dès leur réception et dès la disponibilité dudit serveur.

L'interface de gestion coordonne l'exécution n même temps ou périodiquement et pour chaque poste de personnalisation au moins les types de tâches suivantes :

. surveillance de la survenance d'une requête,

. surveillance de la disponibilité de chaque serveur,

. transmission de la requête à un serveur dès sa disponibilité,

. réception des données de réponse à la requête,

. transmission des données de réponse au poste de personnalisation requérant dès leur réception.

Cette interface de gestion comprend :

- un ordinateur équipé d'une carte multivoies,

- chaque serveur de données et chaque poste de personnalisation étant respectivement connecté à l'ordinateur par une liaison série de la cart multivoies,

- un système d'exploitation temps réel multitâches pour exploiter lesdites tâches en même temps et en temps réel.

Ainsi, ce système permet pour un site de production de déterminer les besoins nécessaires et suffisants en serveur de données par rapport à un objectif de rentabilité ou de productivité. En effet, dans l'art antérieur, pour atteindre un même objectif, il était inévitable d'avoir des serveurs de données en excès, ce qui peut être très onéreux.

L'invention permet en outre :

- d'interfacer tous types de machines venant de différents constructeurs et ayant des configurations de communications différentes ;

- d'optimiser au maximum le partage de ressources externes au procédé de personnalisation, à savoir :

. Serveur de données,

. Boîtes "noires" de chiffrement,

. Tout autre périphérique nécessaire à la personnalisation électrique (Module de contrôle d'accès notamment sous forme de carte à puce ...).

- d'optimiser au maximum le partage de ces ressources vers une ou plusieurs machines de personnalisation ;

- de séparer physiquement le serveur de données (qui peut être physiquement dans une aire très sécurisée, et dialoguer avec le serveur de données/interface de gestion en message sécurisée).

Ce serveur de données/interface de gestion est basé sur un système PC temps réel qui est "cascadable", ce

qui signifie que plusieurs interfaces de gestion peuvent être connectées ensemble en cascade par réseau local. Il est ainsi possible d'augmenter la puissance du système de personnalisation, le système d'exploitation d'une interface de gestion pouvant gérer l'ensemble directement. Cette aptitude est particulièrement avantageuse car elle confère au système de personnalisation une très grande flexibilité.

D'autres caractéristiques et avantages de la présente invention apparaîtront à la lecture de la description suivante d'un exemple particulier de réalisation, ladite description étant faite en relation avec le dessin joint dans lequel :

- la figure 1 est un schéma fonctionnel d'un système de personnalisation de cartes à puces selon l'invention, et
- la figure 2 est un schéma d'un dispositif qui permet de transformer un connecteur en deux liaisons informatiques de type série.

Un système de personnalisation de cartes à puce selon l'invention comprend, par exemple, quatre machines de personnalisation MP1 à MP4 qui sont chacune connectées à un serveur de données SD par des liaisons informatiques de type série LS.

Chaque machine de personnalisation MP1, MP2, MP3 ou MP4 de cartes à puce CP comprend, par exemple pour la machine MP1,

- par exemple six lignes ou postes de personnalisation PP1 à PP6 en parallèle pour personnaliser simultanément six cartes à puce CP1 à CP6,

- un dispositif de contrôle DC contenant les données de personnalisation de chaque carte à personnaliser,

- un bus de communication BC pour transmettre à chaque poste de personnalisation PP1 à PP6 les données de personnalisation de chaque carte à puce CP1 à CP6 fournies par le dispositif de contrôle DC,

- des liaisons informatiques de type série LS1 à LS6, au moins une par poste de personnalisation, pour transmettre à chaque poste de personnalisation les données cryptographiques de chaque carte en cours de personnalisation.

Chaque poste de personnalisation PP1 à PP6 comprend :

- un lecteur/encodeur référencé LE1 pour le poste PP1 et LE6 pour le poste PP6, ce lecteur/encodeur, plus communément appelé lecteur, étant par exemple celui commercialisé par la demanderesse sous le vocable GCI400DC,

- un microprocesseur, référencé TBP1 pour le poste PP1 et TBP6 pour le poste PP6, chaque microprocesseur comportant deux liaisons informatiques de type série, l'une LS1 à LS6 vers le serveur de données SD et l'autre LL1 à LL6 vers le lecteur/encodeur.

Le serveur de données SD comprend :

- un calculateur tel qu'un ordinateur personnel PC qui est équipé d'une carte multivoies CM, système temps réel multi-tâches,

- par exemple six dispositifs périphériques de cryptage DEP1 à DEP6, les initiales DEP étant l'acronyme pour l'expression anglo-saxonne "DATA ENCRYPTION PERIPHERAL", ces dispositifs périphériques DEP1 à DEP6 sont connectés chacun au calculateur PC par une liaison série LD1 à LD6 de la carte multivoies CM.

Dans le schéma de la figure 1, le serveur de données SD est prévu pour gérer quatre machines d personnalisation MP1 à MP4 comportant chacune six postes de personnalisation, chaque poste de personnalisation étant connecté par une liaison série LS à une entrée de la carte multivoies CM.

L'ordinateur PC a pour fonction de gérer les demandes en données cryptographiques de chaque poste de personnalisation en s'adressant aux dispositifs périphériques DEP1 à DEP6 par les liaisons série LD1 à LD6 et en transmettant les données cryptographiques à l'appareil de personnalisation par les liaisons série LS1 à LS6.

Dans cet exemple de réalisation, chaque microprocesseur TBP est équipé de deux liaisons série LS, l'une LS vers le calculateur PC et l'autre LLE vers le lecteur/encodeur LE. Cependant, dans le cas où le microprocesseur TBP n'est pas équipé de deux liaisons série mais d'un connecteur COS à huit conducteurs par exemple, certains de ces conducteurs peuvent être utilisés pour réaliser des liaisons série en utilisant un dispositif d'adaptation DA qui comprend deux adaptateurs pour liaison série SLA1, SLA2 et un circuit de commutation RS selon le schéma de la figure 2.

Sur cette figure 2, on a représenté les huit bornes d'un connecteur de sortie COS comprenant :

- une borne RST pour la remise à zéro,
- une borne V_{pp} pour la tension de programmation,
- une borne V_{cc} pour la tension d'alimentation,
- une borne CLK pour le signal d'horloge,
- une borne I/O pour les signaux de données,
- une borne GNP pour le potentiel de masse,
- une borne FUSE 1 pour un premier fusible de programmation,

- une borne FUSE 2 pour un deuxième fusible de programmation.

Pour réaliser une seule liaison série, les bornes CLK, I/O, V_{cc} et GND sont connectées à un adaptateur qui fournit les signaux série sur deux bornes de sortie Rx et Tx.

Pour réaliser deux liaisons série, les bornes CLK et I/O sont connectées à un double commutateur RS dont la position est commandée par le signal sur la borne V_{pp}. Un premier commutateur RS1 est connecté à la borne horloge CLK par sa borne d'entrée et aux bornes d'entrée CLK de deux adaptateurs SLA1 et SLA2 par ses deux bornes de sortie. Un deuxième commutateur RS2 est connecté à la borne I/O par sa borne d'entrée et aux bornes d'entrée I/O des deux adaptateurs SLA1 et SLA2 par ses deux bornes de sortie.

La borne V_{pp} est connectée aux deux commutateurs RS1 et RS2 tandis que les bornes Vcc et GND sont connectées aux adaptateurs SLA1 et SLA2. Ces adaptateurs SLA1 et SLA2 ont chacun deux bornes de sortie Rx1, Tx1 et Rx2 et Tx2 qui réalisent, par exemple respectivement, la liaison série LS avec le serveur SD et la liaison série LLE avec le lecteur/encodeur LE.

Comme il est connu, la borne Tx1 ou Tx2 est affectée à l'émission du signal tandis que la borne Rx1 ou Rx2 est affectée à la réception du signal.

REVENDICATIONS

1. Système de personnalisation de cartes à puce caractérisé en ce qu'il comprend :

- au moins une machine de personnalisation (MP) équipée chacune d'au moins un poste de personnalisation (PP) émettant des requêtes en données de personnalisation ;
- au moins un serveur de données de personnalisation (SD) délivrant des données de personnalisation ;
- au moins une interface de gestion connectée d'un part à l'une au moins desdites machines de personnalisation (MP) et d'autre part à l'un au moins desdits serveurs de données par une liaison bi-directionnelle, ladite interface de gestion recevant lesdites requêtes, les transmettant à un au moins desdits serveurs, réceptionnant la réponse correspondante, et la transmettant au poste de personnalisation requérant,

caractérisé en ce que ladite interface de gestion est apte à gérer la transmission des sollicitations/requêtes ou besoins en données de personnalisation à l'un au moins desdits serveurs dès leur réception et dès la disponibilité dudit serveur.

2. Système de personnalisation de cartes à puce selon la revendication 1, caractérisé en ce que ladite interface de gestion coordonne l'exécution en même temps ou périodiquement et pour chaque poste de personnalisation au moins les types de tâches suivantes :

. surveillance de la survenance d'une requête,

. surveillance de la disponibilité de chaque serveur,

. transmission de la requête à un serveur dès sa disponibilité,

. réception des données de réponse à la requête,

. transmission des données de réponse au poste de personnalisation requérant dès leur réception.

3. Système de personnalisation de cartes à puce selon l'une des revendications précédentes caractérisé en ce que ladite interface de gestion comporte :

- un ordinateur (PC) équipé d'une carte multivoies (CM),
- chaque serveur de données et chaque poste de personnalisation étant respectivement connecté à l'ordinateur par une liaison série de la carte multivoies (CM),
- un système d'exploitation temps réel multitâches pour exploiter lesdites tâches en même temps et en temps réel.

4. Système selon la revendication 1, 2 ou 3, caractérisé en ce que chaque poste de personnalisation comprend :

- un microprocesseur (TBP),
- un lecteur/encodeur (LE),
- une première liaison informatique de type série (LS) entre le microprocesseur (TBP) et l'ordinateur (PC) du serveur (SD) et,
- une deuxième liaison informatique de type série (LLE) entre le microprocesseur (TBP) et le lecteur-encodeur (LE).

5. Système selon la revendication 4, caractérisé en ce que les première et les deuxième liaisons informatiques de type série (LS, LLE) de chaque microprocesseur (TBP) sont réalisées en connectant certaines bornes de sortie (V_{pp}, V_{cc}, CLK, I/O, GND) d'un connecteur de sortie (COS) du microprocesseur (TBP) à un dispositif d'adaptation (DA).

6. Système selon la revendication 5, caractérisé en ce que le dispositif d'adaptation (DA) comprend :

- un circuit de commutation (RS) comprenant deux commutateurs (RS1, RS2) dont la borne d'entrée est connectée pour l'un (RS1) à la borne de sortie horloge (CLK) et pour l'autre (RS2) à la borne de sortie des signaux de données (I/O), la commutation étant commandée par un signal de programmation sur la borne de sortie (V_{pp}),
- deux circuits adaptateurs (SLA1, SLA2) dont les deux bornes d'entrée sont connectées chacune à une borne de sortie de chaque commutateur (RS1, RS2), lesdits circuits adaptateurs étant par ailleurs connectés à la borne de sortie (V_{cc}) pour l'alimentation électrique et à la borne de sortie masse (GND) du connecteur de sortie (COS).

7. Système de personnalisation de cartes à puce selon l'une des revendications précédentes, caractérisé en ce que ledit serveur est un serveur de données de chiffrement.

8. Système de personnalisation de cartes à puce selon l'une des revendications précédentes caractérisé en ce qu'il comprend un dispositif de contrôle (DC) pour fournir des données supplémentaires de

personnalisation, ledit dispositif étant connecté par l'intermédiaire d'un bus de communication (BC) à chaque poste de personnalisation (PP) d'une machine de personnalisation.

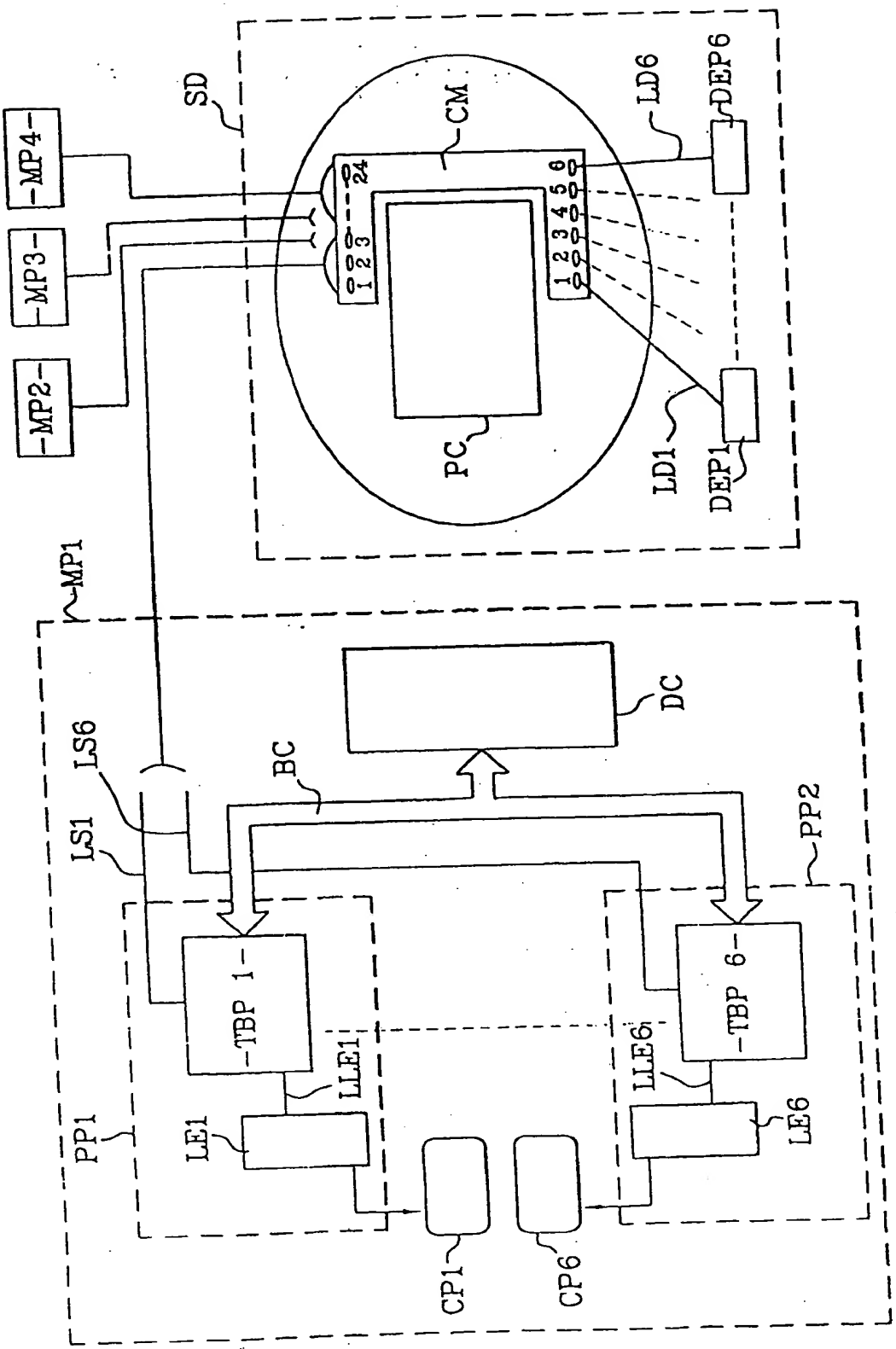
SD
CM
LD6
DEP6
MP4
MP3
MP2
PC
LD1
DEP1
MP1
DC
LS6
BC
LS1
PP2
TBP 1
TBP 6
LLE1
LLE6
LE1
LE6
PP1
CP1
CP6

FIG.1

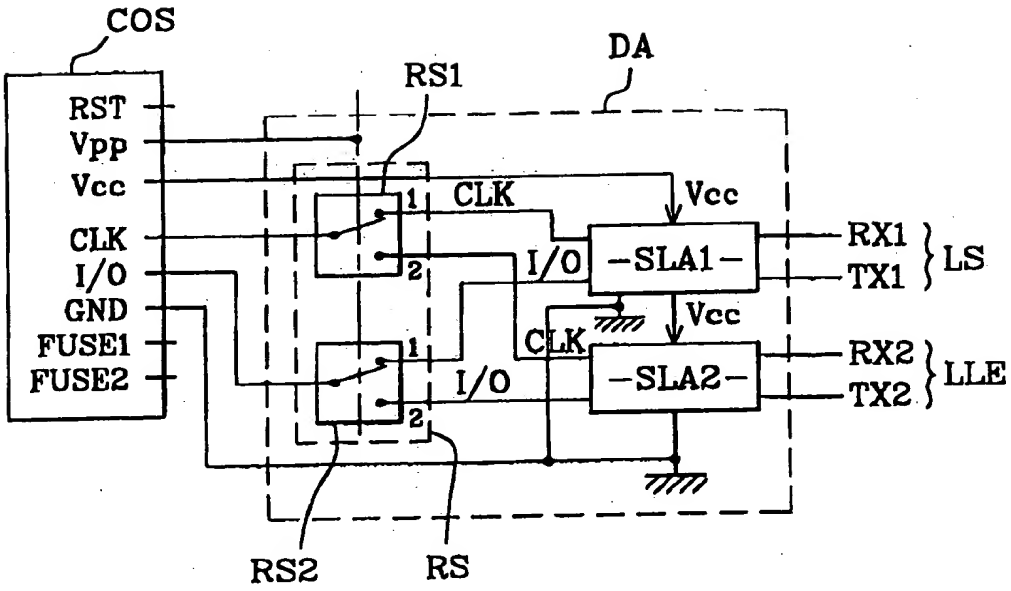
COS
RST
Vpp
Vcc
CLK
I/O
GND
FUSE1
FUSE2
RS1
DA
CLK
Vcc
I/O
-SLA1-
RX1
TX1
LS
Vcc
CLK
I/O
-SLA2-
RX2
TX2
LLE
RS2
RS

FIG.2

THIS PAGE BLANK (USPTO)